ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

July 30, 2012

REPLY COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION, COMMON SENSE MEDIA, CONSUMER WATCHDOG, PRIVACY RIGHTS CLEARINGHOUSE, AND PRIVACY TIMES,

To

THE FEDERAL COMMUNICATIONS COMMISION

Privacy and Security of Information Stored on Mobile Communications Devices

CC Docket No. 96–115; DA 12–818 (77 Fed. Reg. 35336)

The Electronic Frontier Foundation ("EFF"), Common Sense Media, Consumer Watchdog, Privacy Rights Clearinghouse, and Privacy Times[1] submit these reply comments in response to the above-captioned notice published on June 13, 2012. In its notice, the Federal Communications Commission ("FCC") sought comments on "privacy and data security practices of mobile wireless services providers with respect to customer information stored on their users' mobile communications devices."[2] EFF's initial individual comments focused on the practices associated with the mobile wireless services providers' use of Carrier IQ; in these joint reply comments, we focus on the statutory meaning of customer proprietary network information ("CPNI") in light of Carrier IQ.

In their initial comments, *CTIA–The Wireless Association, Verizon, Sprint, AT&T,* and the *Interactive Advertising Bureau* not only urge the FCC to defer making a decision on whether

---

[1] Respectively, https://www.eff.org, https://www.commonsensemedia.org, http://www.consumerwatchdog.org/, https://www.privacyrights.org, and http://www.privacytimes.com.
[2] https://www.federalregister.gov/articles/2012/06/13/2012-14496/privacy-and-security-of-information-stored-on-mobile-communications-devices.

454 Shotwell Street • San Francisco, CA 94110 USA
v +1 415 436 9333 f +1 415 436 9993 i www.eff.org e information@eff.org

information stored on customers' mobile devices should be considered customer proprietary network information ("CPNI"), but also attempt to define away their obligations to keep such information confidential at all. Accepting the limited definition of CPNI that carriers desire would have grave ramifications for consumer privacy in the mobile ecosystem. First, as EFF explains below, the proffered definitions of CPNI are not based in either the statutory text or in the legislative history. Rather, the plain meaning of the term "CPNI" as currently defined encompasses most, if not all, of the information stored on mobile communications devices. Second, the FCC, as a matter of policy, is not obligated to refrain from regulating in this area while carriers await the outcome of a long and arduous multi-stakeholder initiative.

Information Stored on Consumers' Mobile Devices Can Be CPNI

In pertinent part, the statute defines CPNI as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[3]

Sprint, alone among the carriers, argues that the information stored by consumers on their mobile devices is not CPNI, alleging, "Remote diagnostic information is not CPNI, because it does not relate to the quantity, technical configuration, type, destination, location, or amount of use of a telecommunications service subscribed to by a customer."[4]

If Carrier IQ is relevant here, however, the opposite would seem to be true. A June 8, 2011 Carrier IQ press release explains: "Carrier IQ's technology provides mobile network operators and device manufacturers with invaluable insights into the performance of various

---

[3] 47 U.S.C. § 222(h)(1)(A).
[4] Sprint Comments at 12.

devices and networks from the user's perspective."[5] The same document reports: "In a recent operator rollout of Carrier IQ's application analytics, we were able to demonstrate that if Facebook was preloaded on a specific smartphone, 40% of the app usage from that device in the first month was with Facebook. Without the preload, it was only 5%, as users had to download the app themselves."

A 2009 document from Carrier IQ proudly touts one of its products, Experience Manager, as allowing mobile providers to: "Identify exactly how your customers interact with services and which ones they use. See which content they consume, even offline. Identify problems in service delivery, including the inability to connect to the service at all."[6]

If these claims are valid, then the data gathered by Carrier IQ on behalf of the carriers relates to the quantity, technical configuration, type, destination, location, and amount of use of telecommunications service by a customer.

Sprint also argues that the data at issue in this proceeding must be "linked to individual users,"[7] a claim echoed by CTIA and IAB and which would require CPNI to contain "personally identifiable call data."[8] The plain text of Section 222 does not require CPNI to be linked to identified individual users.[9] Nor does it require, as CTIA suggests, that CPNI relate "to whom,

---

[5] http://www.carrieriq.com/documents/8-june-2011-carrier-iq-launches-application-analytics-module-for-global-mobile-operators-and-device-manufacturers/5597/.
[6] The document "ExperienceManager.datasheet-1.pdf" is available at http://www.carrieriq.com/documents/25-march-2009-carrier-iq-adds-experience-manager-to-analytics-products/5589/.
[7] *Id.*
[8] CTIA Comments at 7.
[9] *Contrast* 47 U.S.C. § 222(h)(1) (defining CPNI as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship") *with* IAB Comments at 5 ("[T]he use, disclosure, and access requirements apply to *individually identifiable* customer proprietary network information.").

where and when a customer places a call" or the "services purchased by the customer."[10] In short, these proffered interpretations of Section 222 find no basis in the text of the statute.

That the main CPNI non-disclosure requirements imposed by Section 222(b)(1)(A) apply to "individually identifiable" CPNI[11] seems irrelevant given that the carriers themselves describe "remote diagnostics" as "device-specific."[12] The carriers can associate the device with the subscriber, and it would prove too much if "individually identifiable" did not include "device-identifiable." And if the data gathered by Carrier IQ is representative of the general issue, and Carrier IQ's technology allows companies to "See which content they consume," carriers may even be able to identify different users of a shared device, e.g. different Facebook accounts accessed on one smartphone or tablet.

Even assuming that the information on consumers' mobile devices is not "identifiable," it is still covered by a general obligation to protect customer proprietary information.[13] Section 222 anticipates that carriers will have differing obligations to protect customer data depending on the form that data takes, but does not exclude some forms of customer data altogether.[14] Whether and how industry actors choose to use locally stored consumer information is significant, as aggregated, anonymized customer information is subject to entirely different

---

[10] CTIA Comments at 9.
[11] 47 U.S.C. § 222(b)(1)(A) ("Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to *individually identifiable* customer proprietary network information…") (emphasis added).
[12] Sprint Comments at 12.
[13] 47 U.S.C. § 222 (a) (2012) ("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of. . . customers.").
[14] *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 F.C.C. Rcd. 6927, 6930 (Apr. 2, 2007) ("The section 222 framework calibrates the protection of such information [obtained by virtue of providing a telecommunications service] from disclosure based on the sensitivity of the information.").

statutory constraints than is CPNI.[15] While CTIA suggests that the Commission "lacks statutory authority"[16] to regulate customer data that is not CPNI, the text of Section 222 indicates that the Commission is empowered to regulate carriers' uses and disclosures of aggregate customer information as well as CPNI and subscriber list information.[17]

At the same time, the factual record on the means, methods, and reasons for the gathering of network diagnostic data remains so incomplete that in order to determine whether the information stored on consumers' mobile devices is CPNI, advocates must rely on the carriers' own statements about how they intend to use that data. These uses seem not to be universal across the industry. While Sprint Nextel contends that its collection "generally involve[s] de-identified data used to produce de-identified and aggregated reports so that we can better understand shared performance issues,"[18] neither AT&T nor Verizon attest that they aggregate, anonymize, or otherwise de-identify the data in any way. It is not enough to rely on companies' unilateral assertions that their uses of customer information are innocuous when those uses are opaque to consumers and to regulating authorities.

Nor does the fact that customers enter information on their mobile devices automatically remove that information from the scope of Section 222. Sprint alleges that "most of the data on the device is either entered into the device by consumers or generated through a consumer's interaction with a mobile app."[19] Sprint therefore maintains that customer-generated information can never be CPNI. Similarly, CDT argues that the potential for information to be accessed by non-carriers "diminishes the argument that the data Carrier IQ obtains is made available 'solely

---

[15] 47 U.S.C. § 222(h)(2) (2012) (defining "aggregate customer information" as "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed").
[16] CTIA Comments at 3.
[17] 47 U.S.C. § 222(h)(2)-(3).
[18] Sprint Comments at 2.
[19] Sprint Comments at 13–14.

by virtue of the carrier-customer relationship.'"[20] These interpretations lack any basis in the text of Section 222, which says little about the origins of CPNI. The proportion of information that is actually generated by consumers, accessed by entities other than carriers, or shared by carriers with other entities remains obscure. Moreover, there is no obvious legal reason that information generated by customers or accessed by mobile apps or other actors would not be CPNI if it pertains to the quantity, technical configuration, amount of use, or other factors bearing on usage of communications networks and other carrier services. For this reason, it is our position that the factual record on how information is generated, collected, aggregated, and shared in the mobile environment bears refreshing.

Finally, we question claims made by both the CTIA and Sprint Nextel that the Stored Communications Act (SCA) bars the FCC from exercising its jurisdiction in this area. The SCA generally permits carriers to collect or use information, but also generally restricts the circumstances in which the carriers may share or disclose that information.[21] The CTIA alleges that the SCA provides carriers with "independent authority" to divulge information incident to the provision of services. However, if the CTIA's interpretation were correct, there would be no limitation on the information that the carriers could permissibly divulge; in contrast, Section 222 clearly anticipates that carriers may use information they collect from consumers, but places restrictions on how carriers share that information. We note that carriers' use of information gleaned from consumers' mobile devices is not at issue in this proceeding. Rather, determining whether such information is CPNI bears only on the legal obligations surrounding disclosure.

---

[20] CDT Comments at 8.
[21] 18 U.S.C. § 2702(c).

The FCC is Capable of Regulating Carriers' Uses of Customer Information

As a matter of policy, the FCC is not obligated to refrain from regulating carriers while the NTIA multi-stakeholder process goes forward.[22] The carriers and their advocates fixate on the NTIA multi-stakeholder process as providing a "single, comprehensive" approach to regulating the mobile ecosystem.[23] However, as the Internet Commerce Coalition notes, the NTIA process has only recently begun, and its outcome is as of yet highly uncertain.[24] While the multi-stakeholder process may address the privacy of consumers' locally stored information at some point, it is not clear when, how, or by what means consumers may expect their information to be protected. As AT&T points out, "Rules that apply only to a shrinking subset of mobile services fail to offer consumers a uniform approach to privacy and security."[25] Their solution? Wait to solve consumer privacy problems until the conclusion of NTIA's multi-stakeholder process.

We believe that the FCC can play a vital role in encouraging carriers to participate fruitfully in the NTIA process. Regulation by government agencies is crucial to the success of any self-regulatory regime.[26] Neither the carriers nor their advocates offer any specific reason why the FCC's enforcement of existing rules would derail the "development of voluntary codes of conduct on a broad range of mobile (and other) privacy issues"[27] or "squash" the multi-stakeholder initiative.[28] IAB suggests that "any expansion of a telecommunications carrier's duty under Section 222(a) will result in inconsistency in the mobile marketplace, as well with as

---

[22] Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct, Docket No. 120214135–2135–01 77 Fed. Reg. 13098 (Mar. 5, 2012).
[23] AT&T Comments at 8.
[24] Internet Commerce Coalition Comments at 2.
[25] AT&T Comments at 8–9.
[26] *See generally* Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543 (2000).
[27] AT&T Comments at 4; see also Verizon Comments at 2 ("A code of conduct, such as that under consideration in NTIA's multi-stakeholder process, is the best method to address these issues.").
[28] CTIA Comments at 5.

[*sic*] the FCC's prior decisions, with the adverse consequence of stifled innovation."[29] However, IAB misconstrues the issue at stake in this proceeding, which is not the expansion of current duties but rather the application of existing law to carriers' existing practices.

Carriers' arguments that FCC should not exercise its (lawful) authority in this sphere could easily be extended to information that the FCC has already deemed to be CPNI in a manner that adversely affects carriers. For example, in 1999 Congress amended Section 222 to include customer location information as CPNI. While carriers are now obligated to safeguard customer location information, other entities in the mobile ecosystem are subject to different rules on locational privacy. AT&T suggests that "customers today often expect their devices to be 'location aware' to provide the location-based services they desire" but that consumers "are not cognizant of fine legal distinctions between telecommunications services and other types of services as they choose among the wide variety of service offerings that are available to them. . . ."[30] By asserting that consumers want their location information to be shared and do not know or care who does the sharing, AT&T begs the question of what the appropriate constraints on location sharing ought to be—and ignores the fact that carriers have already been subjected to higher standards in this area than have other actors.

Indeed, carriers seem to argue that subjecting them to the strictures of Section 222 is "unfair" in light of the fact that other actors in the communications industry face different statutory regimes and different sanctions for violations. Nonetheless, the heightened standards of Section 222 have existed since 1996; none of the commenters have shown a direct relationship between the enforcement of Section 222 over the last sixteen years and the purported harm of

---

[29] IAB Comments at 5.
[30] AT&T Comments at 6–7.

stifled innovation. Indeed, carriers repeatedly misconstrue consumers' concerns as limited solely to the collection and use of information by carriers.

In this proceeding, however, we are primarily concerned not with stifling the usage of information retrieved from consumers' mobile devices, but with protecting that information from the type of wrongful disclosure and abuse that prompted the FCC to adopt its pretexting guidelines in 1998. By asking the FCC to withhold judgment on whether information stored locally by consumers can ever amount to CPNI under existing law, carriers and their advocates are asking for a free license to trade and traffic in information that they gain by virtue of performing network diagnostics and other maintenance tasks. Consumers cannot be expected to wait for the outcome of a protracted multi-stakeholder process in order for locally stored information to have any protection from disclosure.

Finally, by ruling on this issue, the Commission would not of necessity hamper innovation or otherwise stifle free enterprise. The Commission may "on its own motion issue a declaratory ruling terminating a controversy or removing uncertainty."[31] Indeed, the Commission has previously opted to make declaratory rulings confirming the scope of other disputed statutory terms where to do so would provide "regulatory certainty"[32] or in order to clarify the relationship between Section 222 and another statute.[33] By issuing a declaratory ruling, the Commission could address carriers' concerns about the manner in which the Stored

---

[31] 47 C.F.R. § 1.2.

[32] *See, e.g.*, *In the Matter of Appropriate Regulatory Treatment for Broadband Access to the Internet Over Wireless Networks*, 22 F.C.C. Rcd. 5901 (Mar. 23, 2007) (defining the statutory classification of a "wireless broadband Internet access service").

[33] *See, e.g.*, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 21 F.C.C. Rcd. 9990 (Aug. 30, 2006) (clarifying "how telecommunications carriers' privacy duties under section 222 affect the requirement that suspected images of child pornography be reported to the CyberTipLine"); *see also In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 25 F.C.C.R. 14335 (Oct. 12, 2010) (clarifying carriers' privacy duties in light of child pornography reporting requirements that superseded those previously issued).

Communications Act intersects with Section 222 and provide clarity on the scope of CPNI in the context of rapidly changing mobile technology. Issuing a declaratory ruling in this case would not lead to the parade of horribles anticipated by the carriers, but could assure their customers that their information is being adequately protected while consumers and the telecommunications industry await the outcome of the NTIA multi-stakeholder process.

It is the FCC's role to maintain the high standards Congress imposed upon carriers through enacting Section 222 and, in so doing, to support the multi-stakeholder process and facilitate self-regulation by AT&T, Sprint Nextel, Verizon, and their counterparts. Indemnifying carriers for trafficking in locally stored information while consumers wait for holistic regulation would be antithetical to both the text and the spirit of Section 222.

ELECTRONIC FRONTIER FOUNDATION

Lee Tien

COMMON SENSE MEDIA

Guilherme Roschke

CONSUMER WATCHDOG

John Simpson

PRIVACY RIGHTS CLEARINGHOUSE

Beth Givens

PRIVACY TIMES

Evan Hendricks